APPENDIX D: CYBERTERRORISM

APPENDIX D: CYBERTERRORISM

Ours is an age of computers, of automated information systems. We are able to access, distribute, and store incredibly large quantities of information in very little time. It is said that information is power. However, our dependence on automated information systems goes much deeper than power-wielding. Virtually all of the infrastructure and the institutions on which we depend—the government, military, communications systems, transportation, utilities, financial systems, emergency medical services, and more—depend on automation. In the financial world, for example, very few transactions actually involve the physical transfer of money; what we transfer is information *about* money.

As we have harnessed automation and created systems to facilitate and quicken our private, corporate, and governmental transactions, those systems have become increasingly vulnerable. We now face the danger of having our information infrastructures destroyed, altered, or incapacitated. Too often those vulnerabilities go unnoticed until disruption or catastrophe occurs.

Attacks on our information systems may come from a wide range of potential aggressors, from other nations to teenage hackers. One of the greatest threats comes from cyberterrorism.

WHAT IS CYBERTERRORISM?

Cyberterrorism is the convergence of ***cyberspace*** (the computer-based world of information) and ***terrorism*** (premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents).

The boundaries of cyberterrorism—what does and what does not constitute an act of cyberterrorism—are variously defined. Here is one definition:

CYBERTERRORISM (CONTINUED)

WHAT IS CYBERTERRORISM? (CONTINUED)

Definition: Cyberterrorism

Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Further, to qualify as cyberterrorism, an attack should *result in violence against persons or property, or at least cause enough harm to generate fear*. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[1]

Cyberterrorism is distinct from computer crime, economic espionage, and "hactivism," although terrorists may employ any of these forms of computer abuse to further their agendas.

The weapons of cyberterrorism—computers—differ from weapons of mass destruction such as biological agents, chemical agents, and radiological agents in that they don't *directly* cause death and injury. However, acting indirectly, they can cause serious consequences to individuals, businesses, industry, government, and the public at large. Depending on how they are used, they can lead to injury and death.

To better understand cyberterrorism, it is helpful to understand the terminology that has been coined to describe this growing phenomenon. The following table provides a few key definitions related to cyberterrorism.

[1] Denning, Dorothy E., "Cyberterrorism." August 2000. Prepublication version of a paper that appeared in *Global Dialogue*, Autumn 2000.

CYBERTERRORISM (CONTINUED)

WHAT IS CYBERTERRORISM? (CONTINUED)

SOME GENERAL TERMS RELATED TO CYBERTERRORISM[2]	
antiterrorism	Defensive measures against terrorism.
counterterrorism	Offensive (proactive) measures against terrorism.
cybercrime	Use of computers to carry out fraud, embezzlement, copyright infringement, scams, and other illegal activities.
cyber-deterrence	Integration of conventional forces, technological exhibitionism, and strategic simulations as a deterrent to enemy aggression.
cyberterrorism	Computer-based, information-oriented terrorism.
cyberwar	Information-oriented warfare waged by formal military forces.
cybotage	Acts of disruption and destruction against information infrastructures; computer sabotage.
cyboteur	One who commits cybotage; anarchistic or nihilistic computer hacker; computer saboteur.
hacking	Breaking into computer networks.
hactivism	Use of hacking by social activists with the intent of disrupting normal operations but not causing serious damage.
information warfare	When broadly defined, this term refers to the use of technology against technology, to deny some entity the ability to use its own technology and its information. Information warfare may be waged against industries, political spheres of influence, global economic forces, or countries. When narrowly defined, this term refers to military uses of information technology.
infosphere	The totality of all information media, especially those that are interconnected and internetted.
netwar	Information-oriented conflict waged by networks of primarily nonstate actors. (Some authors restrict the definition of netwar to information-related conflict at a grand level between nations or societies. Others broaden it to include attacks on private or corporate systems or a city's infrastructure.)

[2] From "Terrorism Evolves Toward Netwar," in Rand Review Winter 1998-99 issue; and Denning, Dorothy E., "Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy* . Arquilla, John, and Ronfeldt, David, eds. Rand Corp., 2001. Both accessed at www.rand.org/publications/randreview/issues/rrwinter98.9/madness.html.

CYBERTERRORISM (CONTINUED)

WHY CYBERTERRORISM?

Cyberterrorism is the weapon of the weak. It appeals to fringe groups who cannot match the military might of their "oppressors" or perceived enemies. Many terrorist organizations aim to achieve a new "future order" if only by wrecking the present. There are several factors that make cyberterrorism an attractive weapon for terrorists:

- **Vulnerability:** The very linkages that enable information technology (IT) systems to function also provide vulnerable points that can be exploited by terrorists. Our sheer dependence on the systems' functioning as planned is a source of great vulnerability.
- **Fear factor:** The underlying agenda of terrorism is to generate fear through random, seemingly uncontrollable acts of violence. For many people, technology carries with it its own fear factor, stemming from its complexity, incomprehensibility, and seeming uncontrollability. The merger of these two sources of fear is a powerful one.
- **Anonymity:** Boundaries are blurred in cyberspace. The ordinary distinctions between public and private interests, war and crime, and geography are less clear. Viruses can be imported into the U.S. through information networks, telephone lines, or on disk media. A cyberattack can be conducted remotely and anonymously, allowing the attacker to avoid detection and capture. (It is often difficult or impossible to know if your system is under attack and by whom.) Remote capability also complicates the investigation, pursuit, and judicial processes because of differences in international laws.
- **Attention:** Cyberterrorism provides a way to assert identity and command attention. If terrorists choose to forego anonymity, an act of cyberterrorism would likely gain extensive media coverage as well as government and public attention.
- **Availability and low cost:** Availability of the weapons of cyberterrorism and the potential for disruptive effects are rising, while financial and other costs are decreasing. A wide array of easy-to-use software attack tools is readily available without cost from thousands of web sites. For a minimum investment, attacks can be waged that are serious and costly; the terrorists can affect more people at less risk to themselves than with other types of terrorist weapons. "Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."[3]
- **Safety:** This form of terrorism does not require the handling of explosives or bio-chemical agents or a suicide mission.
- **Expertise:** In the last few years, many automated attack tools have appeared on the Internet, making it much easier even for ignorant attackers to cause considerable damage. However, new generations of hackers are growing up with ever more digital capability, and hacker networks are already huge. Hackers and insiders might be recruited by terrorists or become self-recruiting cyberterrorists.

[3] National Research Council, "Computers at Risk," National Academy Press, 1991.

CYBERTERRORISM (CONTINUED)

WHY CYBERTERRORISM? (CONTINUED)

- **Fewer taboos:** Cyberterrorism can be conducted with minimal loss of human life, and there are no global taboos associated with waging war against machines. (However, some terrorist groups have made it clear that they are not deterred by the potential for human carnage, and it is possible to use cyberterrorism to cause human casualties.)

These factors make cyberterrorism an appealing weapon and increase the likelihood that cyberterrorism will only increase in the future. U.S. experts are justifiably concerned about our vulnerability to this type of attack. According to the Center for Strategic and International Studies in Washington, DC, "Cyberterrorists, acting for rogue states or groups that have declared holy war against the United States, are known to be plotting America's demise as a superpower."[4]

METHODS OF ATTACK

RISK FACTORS

There are three key risk factors related to computer systems: **access, integrity**, and **confidentiality**.

The proper functioning of information systems is predicated on restricted access to data and operations, on the integrity (accuracy and timeliness) of the data, and on the confidentiality of information that is intended to remain private.

If unauthorized parties gain access to a system, they can cause damaging actions to occur within the system. If a database is accessed and manipulated, the ripple effect can be enormous; the smallest change in a database can cause huge damage (change one number, and all resulting data becomes unreliable).

If confidentiality is breached, private information may become public and sensitive data may fall into the wrong hands. Theft of passwords and user IDs can enable unauthorized access, and the cycle continues.

[4] Global Organized Crime Project, *Cybercrime, Cyberterrorism, and Cyberwarfare*. Center for Strategic and International Studies, 1998.

METHODS OF ATTACK (CONTINUED)

TYPES OF CYBERTERRORISM

The following are some general types of cyberterrorism:

- **Data destruction or corruption:** Using viruses, installation of malicious code, or other means to damage a system from within. This could include destroying or corrupting files, changing data in a database, or corrupting software programs within the system.
- **Penetration of a system to modify its output:** Embedding code (e.g., Trojan horses or "logic bombs") to perform unauthorized functions at a later time.
- **Theft:** System penetration with the goal of stealing information or sensitive data (e.g., password cracking and theft, "packet sniffing").
- **Disabling a system:** Disruption of information structures (e.g., using e-mail bombings, spamming, denial-of-service attacks, or viruses) to crash or disable a system.
- **Taking control of a system:** Taking over a system (e.g., an air traffic system, a manufacturing process control system, a subway or train system, a 911 communications system) to use it as a weapon.
- **Website defacement:** Hacking into a website and changing its contents to spread misinformation, incite to violence, generate fear, or create chaos.

Terrorist groups also use websites, chat rooms, and encrypted e-mail to plan physical acts of terrorism, raise funds for terrorism, provide instructions to fellow terrorists, provide instructions on how to build bombs, spread hate propaganda, and recruit members.

METHODS OF ATTACK (CONTINUED)

SOME TOOLS OF CYBERTERRORISM

The following table describes some of the tools that can be used by cyberterrorists to cause disruption and damage.

Cyberterrorism Tools

TOOL	DESCRIPTION
HERF Gun	High Energy Radio Frequency Gun. Directs a blast of high energy radio signals at a selected target to disable it, at least temporarily. A HERF Gun can shoot down a computer, cause an entire network to crash, or send a telephone switch into electronic chaos. Any of these effects can create denial-of-service scenarios. A HERF Gun is simple and easy to build.
EMP/T Bomb	Electromagnetic Pulse Transformer Bomb. Operates similarly to a HERF Gun, but is many times more powerful and causes permanent damage. According to a 1980 FEMA report[5], the following hardware would be most susceptible to failure from EMP: ▪ Computers, computer power supplies, and transistorized power supplies. ▪ Semiconductor components terminating long cable runs (especially between sites). ▪ Alarm systems and intercom systems. ▪ Life support system controls. ▪ Telephone equipment. ▪ Transistorized receivers, transmitters, and process control systems. ▪ Power control systems. ▪ Communications links. Detonated over a dense urban area, EMP/T Bombs could take out all communications and electronic equipment and cause a blackout.
System intrusion	Unauthorized entry into a system (hacking). Can be used for information gathering, information alteration, and sabotage.
Emissions capture	Various tools are available for capturing vital information secrets such as passwords or data. Packet sniffing (below) is one approach. Van Eck emissions enable hackers to capture the contents of computer screens from up to 200 meters away. Devices designed to capture these emissions can be developed at very low cost.
Virus	A program that can attach itself to legitimate files and propagate, spreading like an infectious disease from computer to computer as files are exchanged between them. The virus hides until a certain criterion is met, then attacks the system by erasing files, destroying hard disk drives, or corrupting databases.
Worm	Operates much like a virus but can travel along a network on its own.

[5] FEMA. *EMP Threat and Protective Measures.* Report for public distribution. April 1980, p. 11.

METHODS OF ATTACK (CONTINUED)

SOME TOOLS OF CYBERTERRORISM (CONTINUED)

TOOL	DESCRIPTION
Trojan horse	A program that pretends to be a benign program but is really a program of destruction. When the user runs the program, it can perform the same kind of destruction as a virus.
E-mail bombing	Flooding a site with so many e-mails that the system becomes paralyzed.
Logic bomb	Unauthorized code that creates havoc when a particular event occurs, such as a certain date.
Packet sniffing	Installing a software program on a network that monitors packets sent through the system and captures those that contain passwords and user IDs.
Spamming	Flooding a system with massive numbers of a message.
Sustainable pulsing	Repeated convergence, redispersion, and recombination of small, dispersed, internetted forces against a succession of targets.
Swarming	Unleashing multiple attacks on a cyberspace target from all directions at once.
Denial-of-service attack	Causing internal damage to a server, or overloading a site with “hits,” to the extent that service is denied to authorized users.
Web sit-in	Mass convergence on a website to overload the site (e.g., with rapid and repeated download requests).

POTENTIAL TARGETS OF CYBERTERRORISM

Of greatest concern for emergency planners are terrorist attacks intended to interfere with national life support systems. Systems of greatest priority include:

- Telecommunications.
- Banking and finance.
- Electrical power.
- Oil and gas distribution and storage.
- Water supply.
- Transportation.
- Emergency services.
- Government services.

Even worse would be the simultaneous occurrence of a physical act of terrorism, such as release of a chemical or biological agent or detonation of a radioactive device, and an act of cyberterrorism that would interfere with response capabilities.

METHODS OF ATTACK (CONTINUED)

POSSIBLE CYBERTERRORISM SCENARIOS

Many potential scenarios for cyberattacks have been suggested, and there are undoubtedly many more that are equally possible. The following are some of the scenarios that have been discussed in cyberterrorism literature, along with selected examples of actual events that have occurred. Although safeguards are in place that would make some of these scenarios very difficult, the range of potential cyberterrorist scenarios indicates the extent of our vulnerability.

- **Power grid:** Attack the computer systems that control a large regional power grid. If the power is lost for a sustained period of time, people may die. Most life support, emergency response, law enforcement, HVAC, and other systems depend on electrical power.) If a nuclear reactor is located in the region, a meltdown may occur, causing a major radiological incident that could cause mass casualties. (See Appendix C for more information on nuclear power plant incidents.)

> **Fact:** *The U.S. power system is divided into four electrical grids supplying Texas, the Eastern States, the Midwestern States, and the Northwestern States. They are all interconnected in Nebraska. A unique aspect of the electrical grids, as with communication grids, is that most built-in computerized security is designed to anticipate no more than two disruptions concurrently. In other words, if a primary line went down, the grid would ideally shut off power to a specific section while it rerouted electricity around that problem area. If it ran into two such problems, however, the grid is designed to shut down altogether.*[6]

- **Air traffic:** Break into an air traffic control system and tamper with the system in such a way that airplanes collide, resulting in mass death; or disable landing systems.

> **Fact:** *In one documented incident, someone took control of the computer system at a small U.S. airport and switched off the landing lights. This action could have killed many people.*

- **Subway/train system:** Take over the operation of a subway or train system, to similar effect.

> **Fact:** *In Japan, groups have attacked the computerized control systems for commuter trains, paralyzing major cities for hours.*

[6] Bowman, Stephen. *When the Eagle Screams: America's Vulnerability to Terrorism.* New York: Carol Publishing Group, 1994, p. 125. As quoted in Devost, Matthew G. *National Security in the Information Age.* University of Vermont Masters Thesis, May 1995. Accessed at: www.terrorism.com/documents/devostthesis.html.

METHODS OF ATTACK (CONTINUED)

POSSIBLE CYBERTERRORISM SCENARIOS (CONTINUED)

- **Financial and business systems:** Disrupt banks, international financial transactions, and stock exchanges. Economic systems grind to a halt, the public loses confidence, and destabilization is achieved.

> **Fact:** *It costs a billion dollars and takes six weeks to recover from a one-day bank failure. If Wall Street suddenly closed down, the United States would lose hundreds of billions of dollars.)*

- **Communications systems:** Invade public telephone networks, shutting down major switching hubs and disrupting emergency 911 services. Or invade the wireless networks on which we have become increasingly dependent. Extended denial-of-service could paralyze business, government agencies, airports, and some military installations.

> **Fact:** *Hackers have invaded the public phone networks, compromising nearly every category of activity, including switching and operations, administration, maintenance, and provisioning. They have crashed or disrupted signal transfer points, traffic switches, and other network elements. They have planted "time bomb" programs designed to shut down major switching hubs, disrupted emergency 911 services throughout the Eastern seaboard, and boasted that they have the capability to bring down all switches in Manhattan.*

- **Critical communications hubs:** Disable telephone company computers that service airports, fire departments, and other communications-dependent services.

> **Fact:** *In March 1997, a hacker in Massachusetts penetrated and disabled a telephone company computer that services the Worcester Airport. For 6 hours, service was cut off to the FAA control tower, the airport fire department, airport security, the weather service, and several private airfreight companies. The lost service caused financial damages and threatened public health and public safety.*

- **Emergency alert and emergency response:** Disable emergency alert systems, preventing the public from being notified of dangerous chemical releases or other emergencies; scramble the software used by emergency services.

> **Fact:** *A fired employee hacked into Chevron's computer systems, reconfiguring them and causing them to crash, and disabling the firm's alert system. The disabled alert system went undetected until there was a plant emergency involving a noxious release and the system could not be used to notify the adjacent community. Thousands of people in 22 States and areas of Canada were put at risk.*

METHODS OF ATTACK (CONTINUED)

POSSIBLE CYBERTERRORISM SCENARIOS (CONTINUED)

- **Utilities:** Penetrate the computer systems of utilities to cause "accidents" affecting public health and services, compromise systems monitoring the water supply, change pressure in gas pipelines to cause valve failure, or bring down the system.

> **Fact:** *In Australia, someone penetrated a municipal computer system and used radio transmissions to create overflows of raw sewage along the coast.*

- **Process control:** Take over the process control computers in a manufacturing line (e.g., change the formulation of a pharmaceutical or food product to make it unsafe); trigger oil refinery explosions and fires.
- **Military intrusion:** Disrupt military networks. Nearly everything the military does depends on computer-driven civilian information networks.

> **Fact:** *The U.S. Department of Defense websites experience about 60 cyberattacks per week.*

- **Banking extortion:** Attack banking and other financial computer networks. One scenario is to hack into a large bank's computer system and leave a message threatening the bank with various forms of cyberterrorism (e.g., logic bombs or electromagnetic pulses to destroy the bank's files). Unwilling to reveal their vulnerability to the public, the bank might succumb to extortion.
- **Medical systems:** Hack into medical records or pharmacy systems and change vital data, causing dangerous changes in treatments and loss of confidence in the system. Corrupt, disrupt, or crash a hospital's computer system, putting many human lives at stake.
- **Business information systems:** A successful attack on just a few business information systems could cause a severe lag in the American economy.

METHODS OF ATTACK (CONTINUED)

POSSIBLE IMPACT

The potential impact of various scenarios has been described above. The vast majority of past cyberattacks have been nuisance attacks, but experts warn that attacks by true terrorists are a matter of “when,” not “if.” If the apparent coordination and patience employed by the September 11 terrorists were applied to a multifaceted cyberterrorist attack, the results could be catastrophic. Matthew Devost paints this hypothetical picture:

> Imagine a well trained team of saboteurs, operating over several years, infiltrating several high technology companies like Microsoft or Novell, a few major automobile manufacturers, or a couple of airlines. Viruses or trojan horses are timed to detonate on a certain day, rendering computer systems inoperable. A small team of hackers infiltrates large computer, telecommunications, and power centers preparing them for denial of service attacks. Another team constructs several large EMP/T bombs and HERF Guns to be directed at targets like the Federal Reserve and Wall Street. Doomsday arrives, and the country's electronic blood stops flowing. No transfer of electronic funds, no stock exchange, no communications and power in a majority of locations, no traffic control, no air travel. . . and we have no one to blame.[7]

While this may be an extreme example, it is clear that a cyberattack of much smaller proportions has the potential for serious disruption of local networks and the systems on which emergency management depends.

THE CLIMATE FOR CYBERTERRORISM

Several emerging changes in organization, strategy, and technology typify the climate for cyberterrorism.

- **Organization:** Terrorists are moving from traditional hierarchical groups toward more flexible network forms or organization—flatter, decentralized designs.
- **Strategy:** While some terrorist groups are moving toward a war paradigm of attacking U.S. military forces and assets, other are replacing destruction of physical targets with disruption of information infrastructures as their objective.
- **Technology:** Terrorists are becoming increasingly dependent on advanced information technologies for offensive and defensive purposes and to support their own organizations. While this may make them disinclined to “take down the Net,” which is their own communication tool, they may be more inclined to use it to wreak havoc on “enemy” infrastructures.

[7] Devost, Matthew. *National Security in the Information Age,* p. 35.

THE CLIMATE FOR CYBERTERRORISM (CONTINUED)

NETWAR

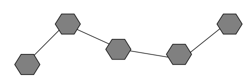
This emerging approach to terrorism, which some authorities refer to as *netwar,* involves using "network forms of organization and related strategies and technologies attuned to the information age. The perpetrators are most likely to consist of small, dispersed groups who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command."[8]

Organizationally, "netwarriors" are likely to be set up as diverse, dispersed "nodes" who share a set of ideas and interests and are arrayed to act in a fully networked manner.

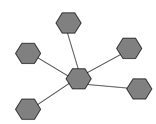
Network Types

There are three basic types of networks, each suited to different conditions and purposes:

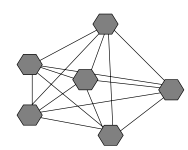
- **Chain network:** People, goods, or information move along a line of separated contacts; end-to-end communication must travel through intermediate nodes. Example: Smuggling chain.



- **Star, hub, or wheel network:** Members are tied to a central node, and all must go through that node to communicate and coordinate with each other. Example: Terrorist syndicate or cartel.



- **All-channel network:** Every group or node is connected to every other group or node. The design is flat: there is no single, central leadership or command and therefore no precise head that can be targeted. Decision making is decentralized, allowing for local initiative and autonomy. Examples: Collaborative network of militant small groups; the al-Qaida network.



The all-channel network is gaining strength from the information revolution. For offense, the design is adaptable, flexible, and versatile, especially for swarming. For defense, these networks tend to be diverse and redundant—difficult to crack and defeat as a whole. If one cell is removed, another can take its place.

[8] The Rand Organization. "Old Madness, New Methods," in Rand Review Winter 1998-99 issue. Accessed at www.rand.org/publications/randreview/issues/rrwinter98.9/madness.html.

THE CLIMATE FOR CYBERTERRORISM (CONTINUED)

WHO ARE LIKELY CYBERTERRORISTS?

Various groups appear to be evolving in the direction of netwar and are potential cyberterrorists. General examples include:

- Transnational terrorist groups.
- Black-market proliferators of weapons of mass destruction.
- Fundamentalist and ethnonationalist movements.
- Back-country militias.
- Militant single-issue groups in the United States.
- Anarchistic and nihilistic leagues of computer-hacking cyboteurs.

Islamic fundamentalist organizations such as Hamas, Osama bin Laden's Arab Afghan network (al Qaida), Algeria's Armed Islamic Group, Hezbollah, and the Egyptian Islamic Group are known to be using information technology to further their objectives.

PROTECTING AGAINST CYBERTERRORISM

In some respects, protection against cyberterrorism is a Federal and international issue. Below are some of the Federal and global actions that have been taken to help protect against cyberterrorism.

The Federal (and Global) Response

1987:	The Computer Security Act of 1987 was passed, requiring Federal agencies to identify systems that contain sensitive information and to develop plans to safeguard them.
1996:	The President's Commission on Critical Infrastructure Protection was established to analyze the vulnerabilities of and threats to critical national infrastructures, including telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. The Executive Order stated that threats include physical threats as well as ***threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats")*** and called for the government and private sector to work together to develop a strategy for protecting them and assuring their continued operation.
1997:	The President's Commission on Critical Infrastructure Protection concluded that the U.S. infrastructure is increasingly vulnerable to attack and that local, State, and Federal officials are not prepared to deal with the problem.
1998:	The National Infrastructure Protection Center (NIPC)—a new FBI command center to fight cyberattacks against the nation's critical computer networks—was established.
1998:	National Security Council aide Richard Clarke was appointed head of the new office on infrastructure protection and counterterrorism. A new U.S. initiative was begun to protect telecommunications systems, banks, telephone networks, air traffic control centers, and other public and commercial networks.
2001:	The Office of Homeland Security was established to integrate and coordinate counterterrorism efforts in the wake of the September 11 attacks. Its mission includes "efforts to protect critical public and privately owned information systems within the United States from terrorist attack."
2001:	An international cybercrime treaty was signed, uniting countries in the fight against computer criminals.

PROTECTING AGAINST CYBERTERRORISM (CONTINUED)

WHAT CAN BE DONE AT THE STATE AND LOCAL LEVEL

The issue at the State and local levels is how to protect critical infrastructure systems from intrusion, attack, damage, and disruption by cyberterrorists.

Reducing Vulnerability

In 1996, the U.S. General Accounting Office (GAO) produced a report[9] on information security and computer attacks at the Department of Defense. Its recommendations for reducing vulnerability to cyberattack include the following steps, which can be effectively applied to all levels of government and all sizes of organization.

1. **Policy:** Clear and consistent information security policies and procedures.

2. **Vulnerability assessment:** Vulnerability assessments to identify security weaknesses at individual installations.

3. **Correction:** Mandatory correction of identified network/system security weaknesses.

4. **Reporting:** Mandatory reporting of attacks to help better identify and communicate vulnerabilities and necessary corrective actions.

5. **Damage assessment:** Damage assessments to reestablish the integrity of information compromised by an attacker.

6. **Awareness:** Awareness training to ensure that computer users understand the security risks associated with networked computers and practice good security.

7. **Expertise:** Assurance that network managers and system administrators have sufficient time and training to do their jobs.

8. **Technical solutions:** Prudent use of technical solutions such as firewalls and smartcards.

9. **Response capability:** An incident response capability to aggressively detect and react to attacks and track and prosecute attackers.

Cyberterrorism should be dealt with as a community matter—that is, through joint cooperative efforts of State and local government, the private sector, and the public.

[9] U.S. General Accounting Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks.* Chapter Report, 5/22/96, GAO/AIMD-96-84. Available at www.fas.org/irp.gao.

PROTECTING AGAINST CYBERTERRORISM (CONTINUED)

System Protections

Currently there are no foolproof ways to protect a system. (A completely secure system could never be accessed by anyone.) However, three broad approaches can be used to reduce vulnerability to cyberterrorism: isolation, encryption, and security.

Isolation	Most military classified information is kept on machines with ***no outside connection***, to prevent unauthorized access to the information. Although this method can protect certain data files, isolation is less effective in protecting a system that by its very nature requires interface with other infospheres. Another approach that is related to isolation is the use of ***firewalls***. Firewalls are hardware and software components that protect one set of system resources from attack by outside network users by blocking and checking all incoming network traffic. A firewall filters access to a network. It may take the form of a computer, router, or other communications device, or it may be a network configuration. A firewall defines the services and access that are permitted to each user. It screens all communications to a system, including e-mail messages (which may carry logic bombs). One firewall method is to screen user requests to check if they come from a previously defined domain or Internet Protocol (IP) address. Another method is to prohibit Telnet access into the system.
Encryption[10]	Encryption is software technology that locks computerized information to keep it private. Only those with an "electronic key" can decipher the information. Encryption does not protect the entire system—only the encrypted data. An attack (e.g., a virus) designed to cripple the whole system is unaffected by encryption.
Security	Security is the protection of information, systems, and services against disasters, mistakes, and manipulation so that the likelihood and impact of security incidents is minimized. Since full isolation is virtually impossible, and encryption is aimed at protecting specific data, not systems, having a program for system security in place is a vital aspect of protecting critical infrastructures.

[10] **Note:** Because terrorists and other criminals are known to have used encryption to conduct illegal activities while avoiding government monitoring (e.g., the mastermind of the 1993 World Trade Center bombing used encryption technology in his foiled plot to blow up 11 U.S. airliners in the Far East), the government has placed some restrictions on the exportation of encryption software and hardware. The U.S. government and the FBI also favor a system whereby the government can gain the key to an encrypted system after gaining a court order to do so. Terrorists in New York City were plotting to bomb the United Nations building, the Lincoln and Holland Tunnels, and the main Federal building. Court-ordered electronic surveillance enabled the FBI to disrupt the plot, and the evidence obtained was used to convict the conspirators.

PROTECTING AGAINST CYBERTERRORISM (CONTINUED)

Defining the Need

Systems with different requirements need to be secured in different ways. For example:

- A system may not contain confidential data but must be available 24 hours a day. This system would have low data sensitivity requirements but ***high availability*** requirements. High availability systems always require better confidentiality to prevent denial-of-service attacks.
- For some systems, ***confidentiality*** (nondisclosure of information) is more important than integrity.
- For others, the need for ***integrity*** (protection against unauthorized modification of information) outweighs confidentiality.

A balance must be found between too much security (very restrictive use, high cost) and too little security (unrestricted use, low visible cost, but high danger). It is important that the value of the information and processes in the system is determined, and the risks identified, so that appropriate countermeasures can be implemented. A cornerstone of countermeasures is ***risk analysis*** and ***security policy***.

Why Develop a Security Policy?

A security policy is a preventive mechanism for protecting important data and processes. It communicates a coherent security standard to users, managers, and technical staff. A policy is important for:

- Measuring the relative security of the current systems.
- Defining interfaces to external partners and users.
- Ensuring that legal requirements are met regarding protection of client and employee data.

Assessing the Security of the System

The following Security Checklist provides a brief glimpse at some of the factors that are typically considered in a security assessment.

PROTECTING AGAINST CYBERTERRORISM (CONTINUED)

SECURITY CHECKLIST	YES	NO
PHYSICAL SECURITY		
1. Is your computing area and equipment physically secured?	☐	☐
2. Are there procedures in place to prevent terminals from being left in an logged-on state, however briefly?	☐	☐
3. Are screens automatically locked after 10 minutes idle?	☐	☐
4. Are modems set to Auto-Answer OFF (not to accept incoming calls)?		
5. Are your PCs inaccessible to unauthorized users (e.g., located away from public areas)?	☐	☐
6. Do your staff wear ID badges?	☐	☐
7. Do you check the credentials of external contractors?	☐	☐
8. Do you have procedures for protecting data during equipment repairs?		
9. Is waste paper binned or shredded?	☐	☐
10. Do you have procedures for disposing of waste material?	☐	☐
11. Do your policies for disposing of old computer equipment protect against loss of data (e.g., by reading old disks and hard drives)?	☐	☐
12. Do you have policies covering laptop security (e.g., cable lock or secure storage)?	☐	☐
ACCOUNT AND PASSWORD MANAGEMENT		
1. Do you ensure that only authorized personnel have access to your computers?	☐	☐
2. Do you require and enforce appropriate passwords?	☐	☐
3. Are your passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?	☐	☐
4. Are your computers set up so that staff entering passwords cannot be viewed by others?	☐	☐

PROTECTING AGAINST CYBERTERRORISM (CONTINUED)

SECURITY CHECKLIST	YES	NO
REMOTE ACCESS		
1. Do you have rules for remote log-on or support that protect against unauthorized intrusion?	☐	☐
2. Are employees aware that transmissions over cellular/wireless phones are not secure?	☐	☐
3. Are dial-up numbers kept confidential?	☐	☐
VIRUS PROTECTION		
1. Do you use, and regularly update, anti-virus software?	☐	☐
2. Do you have a machine dedicated to checking against viruses?	☐	☐
3. Do you have rules about what can and cannot be sent over e-mail and what may and may not be downloaded from the Internet or Bulletin Board Services?	☐	☐
4. Is all new software checked for viruses before installation?		
DATA BACKUP AND RESTORATION		
1. Is individual and department data backed up regularly and after significant changes?	☐	☐
2. Do you have a system for archiving information?	☐	☐
3. Are archives kept in a secure environment?	☐	☐
4. Are Restores regularly tested?	☐	☐
OPERATING SYSTEMS		
1. Are your operating systems updated with current security patches?	☐	☐
APPLICATION SOFTWARE		
1. Is your software certified for security (e.g., according to the Federal criteria or ISO)?	☐	☐
2. Are your common applications configured for security?	☐	☐

PROTECTING AGAINST CYBERTERRORISM (CONTINUED)

SECURITY CHECKLIST	YES	NO
CONFIDENTIALITY OF SENSITIVE DATA		
1. Are you exercising responsibility to protective sensitive data under our control?	☐	☐
2. Is your most valuable or sensitive data encrypted?	☐	☐
DISASTER RECOVERY		
1. Do you have a current disaster recovery plan?	☐	☐
SECURITY AWARENESS AND EDUCATION		
1. Are you providing information about computer security to your staff?	☐	☐
2. Are employees taught to be alert to possible security breaches?	☐	☐

IMPROVING SECURITY

Improving security involves:

- Knowing what data and processes need to be protected.
- Recognizing the threats and judging possible impacts.
- Calculating the risks and deciding what level of risk is acceptable.
- Developing and implementing countermeasures to reduce the risk to an acceptable level.
- Testing and tuning the countermeasure strategy to ensure security.

There are two general ways[11] to approach security improvement: bottom-up and top-down. Each has advantages and disadvantages:

APPROACH	ADVANTAGES	DISADVANTAGES
Bottom-Up	▪ Faster	▪ Not very precise. ▪ Requires advance knowledge of what you want to protect, from whom, and to what degree.
Top-Down	▪ Methodical ▪ More precise	▪ Takes longer ▪ High initial costs

If security needs to be urgently improved, ***both*** methods should be used simultaneously. That is, use the bottom-up approach for important, well-known systems and use the top-down approach to establish a long-term, precise policy and strategy.

BOTTOM-UP APPROACH

The bottom-up approach includes the following steps:

1. Understand your system, including:

   - Current policies.
   - Network topology.
   - Operating procedures.
   - User practices currently in use.
   - What information or processes in the system are most important.

[11] Adapted from Boran, Sean. *IT Security Cookbook*, 2001. Accessed at www.boran.com/security.

IMPROVING SECURITY (CONTINUED)

BOTTOM-UP APPROACH (CONTINUED)

2. Create an attack profile. That is, if you were an attacker, how would you go about attacking the system? (Thinking like an attacker can open surprising possibilities, and hence weaknesses.) Consider:

   - What networks are systems are visible via external network connections, modems, etc.?
   - Where are important systems kept?
   - How physically accessible are they?
   - How would you persuade employees to give you passwords?

3. Summarize weaknesses identified in steps 1 and 2, creating a short list of weaknesses and future threats to be countered.

4. Define an information policy (if not already existing), distribute it to users, and educate them.

5. Create a user policy, distribute it to users, and educate them.

6. Create technical guidelines for the secure installation, maintenance, and production of your servers and networks or other perceived weak points.

7. Audit sensitive systems regularly.

TOP-DOWN APPROACH

There are many ways to conduct a top-down security improvement process. Any such process should be conducted by specialists in information technology security using formal analysis methods. The following process is provided as an example.

1. **Asset analysis:** Conduct an asset analysis (what needs to be protected?). Consider:

   - What are the important assets?
   - Are they stored on computer?
   - What are implications of these assets being compromised, in terms of public safety, emergency response capability, functionality of critical infrastructure, financial loss, etc?

   The measures taken to protect assets should correspond to the value of the assets.

2. **Policy analysis:** Analyze current security rules, policies, and practices (if any).

IMPROVING SECURITY (CONTINUED)

TOP-DOWN APPROACH (CONTINUED)

3. **Objectives:** Define basic security objectives (e.g., availability, confidentiality, and integrity objectives).

4. **Threat analysis:** Identify what threats need to be countered, and their potential sources. Threats tend to be general in nature. Although our focus here is on terrorist threats, any security program would be designed to counter all types of potential threats. See the Threat Checklist later in this appendix for examples.

5. **Impact analysis:** Determine what is the impact or consequence if a threat (or combination of threats) is realized. Consider both short-term and long-term impact. The potential impact can be given a numerical value, as shown on the Threat Checklist.

6. **Risk calculation:** This is a three-part step:

   a. Calculate the likelihood of a threat occurring. Again, the threat likelihood can be given a numerical value, as shown on the Threat Checklist.
   b. Calculate risk (risk = impact x likelihood). If a 0-5 scale was used for both impact and likelihood, risk could have a value ranging from 0 to 25.
   c. Set an acceptable risk value. All risks having a value higher than this number are risks which must be countered. (For example, if the value is set at 15, then all risks having a value higher than 15 must be countered.) **Note:** When dealing with risks that involve public safety, it may not be possible to use a simple acceptable risk value. Presumably, a threat that could affect public safety would be unacceptable.

7. **Constraints analysis:** Examine requirements outside of your control, such as:

   - National and international laws.
   - Agency requirements (mission, strategy, etc.).
   - Budget.

8. **Counter strategy:** Decide on a counter strategy to eliminate or reduce the risk or to limit the potential damage. Consider:

   - Security objectives.
   - Countermeasures (e.g., policy, roles, processes, responsibility, security mechanisms).
   - Feasibility (Can risks be reduced to an acceptable level with this strategy? Are costs acceptable? If not, redo the strategy.)

IMPROVING SECURITY (CONTINUED)

TOP-DOWN APPROACH (CONTINUED)

9. **Implementation:** Put the strategy into practice. Include the following steps:

   a. Develop a security policy and guidelines together with an information classification system.
   b. Define a security organization which clearly defines roles and responsibilities of users, administrators, and managers.
   c. Run pilot tests and revise the system as needed.
   d. Implement the strategy on a broad basis to secure the entire system.
   e. Reevaluate risks and security strategy regularly.

IMPROVING SECURITY (CONTINUED)

THREAT CHECKLIST

This is an example of a threat checklist[12] using 0-5 rating scales for impact and likelihood.

IMPACT SCALE		LIKELIHOOD SCALE	
0	Impact is negligible.	0	Unlikely to occur
1	Effect is minor; major agency operations are not affected.	1	Likely to occur less than once per year
2	Agency operations are unavailable for a certain amount of time, costs are incurred, public confidence is minimally affected.	2	Likely to occur once per year
3	Significant loss of operations; significant impact on public confidence.	3	Likely to occur once per month
4	Effect is disastrous; systems are down for an extended period of time; systems need to be rebuilt and data replaced.	4	Likely to occur once per week
5	Effect is catastrophic; critical systems are offline for an extended period; data are lost irreparably corrupted; public health and safety are affected.	5	Likely to occur daily

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
GENERAL THREATS 1. Human error: ▪ Accidental destruction, modification, disclosure, or incorrect classification of information. ▪ Ignorance: Inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge. ▪ Workload: Too many or too few system administrators; highly pressured users. ▪ Users may inadvertently give information on security weaknesses to attackers. ▪ Incorrect system configuration. ▪ Security policy not adequate. ▪ Security policy not enforced. ▪ Security analysis may have omitted something important, or be wrong.			

12 Adapted from Boran, 2001.

IMPROVING SECURITY (CONTINUED)

THREAT CHECKLIST (CONTINUED)

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
2. Dishonesty: Fraud, theft, embezzlement, selling of confidential agency information. 3. Attacks by “social engineering”: ▪ Attackers may use telephone to impersonate employees to persuade users/administrators to give username/passwords/modem numbers, etc. ▪ Attackers may persuade users to execute Trojan horse programs. 4. Abuse of privileges/trust. 5. Unauthorized use of “open” terminals/PCs. 6. Mixing of test and production data or environments. 7. Introduction of unauthorized software or hardware. 8. Time bombs: Software programmed to damage a system on a certain date. 9. Operating system design errors: Certain systems were not designed to be highly secure. 10. Protocol design errors: Certain protocols were not designed to be highly secure. Protocol weaknesses in TCP/IP can result in: ▪ Source routing, DNS spoofing, TCP sequence guessing, unauthorized access. ▪ Hijacked sessions and authentication session/transaction replay; data is changed or copied during transmission. ▪ Denial of service, due to ICMP bombing, TCP_SYN flooding, large PING packets, etc. 11. Logic bomb: Software programmed to damage a system under certain conditions. 12. Viruses in programs, documents, e-mail attachments.			

IMPROVING SECURITY (CONTINUED)

CHECKLIST (CONTINUED)

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
IDENTIFICATION/AUTHORIZATION THREATS			
1. Attack programs masquerading as normal programs (Trojan horses).			
2. Attack hardware masquerading as normal commercial hardware.			
3. External attackers masquerading as valid users or customers.			
4. Internal attackers masquerading as valid users or customers.			
5. Attackers masquerading as helpdesk/support personnel.			
RELIABILITY OF SERVICE THREATS			
1. Major natural disasters: fire, smoke, water, earthquake, storms/hurricanes/tornadoes, power cuts, etc.			
2. Minor natural disasters, of short duration, or causing little damage.			
3. Major human-caused disasters: war, terrorist incidents, bombs, civil disturbance, dangerous chemicals, radiological accidents, etc.			
4. Equipment failure from defective hardware, cabling, or communications system.			
5. Equipment failure from airborne dust, electromagnetic interference, or static electricity.			
6. Denial of service: ▪ Network abuse: Misuse of routing protocols to confuse and mislead systems. ▪ Server overloading (processes, swap space, memory, “tmp” directories, overloading services). ▪ E-mail bombing. ▪ Downloading or receipt of malicious Applets, ActiveX controls, macros, Postcript files, etc.			

IMPROVING SECURITY (CONTINUED)

CHECKLIST (CONTINUED)

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
7. Sabotage: Malicious, deliberate damage of information or information processing functions. ▪ Physical destruction of network interface devices, cables. ▪ Physical destruction of computing devices or media. ▪ Destruction of electronic devices and media by electromagnetic radiation weapons (HERF Gun, EMP/T Gun). ▪ Theft. ▪ Deliberate electrical overloads or shutting off electrical power. ▪ Viruses and/or worms. ▪ Deletion of critical system files. **PRIVACY THREATS** 1. Eavesdropping: ▪ Electromagnetic eavesdropping/Van Eck radiation. ▪ Telephone/fax eavesdropping (via “clip-on,” telephone bugs, inductive sensors, or hacking the public telephone exchanges. ▪ Network eavesdropping: Unauthorized monitoring of sensitive data crossing the internal network, unknown to the data owner. ▪ Network eavesdropping: Unauthorized monitoring of sensitive data crossing the Internet, unknown to the data owner. ▪ Subversion of DNS to redirect e-mail or other traffic. ▪ Subversion of routing protocols to redirect e-mail or other traffic. ▪ Radio signal eavesdropping. ▪ Rubbish eavesdropping (analyzing waste for confidential documents, etc.).			

IMPROVING SECURITY (CONTINUED)

CHECKLIST (CONTINUED)

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
INTEGRITY/ACCURACY THREATS			
1. Malicious, deliberate damage of information or information processing functions from external sources.			
2. Malicious, deliberate damage of information or information processing functions from internal sources.			
3. Deliberate modification of information.			
ACCESS CONTROL THREATS			
1. Password cracking (access to password files, use of bad (blank, default, rarely changed) passwords).			
2. External access to password files, and sniffing of the network.			
3. Attack programs allowing external access to systems (backdoors visible to external networks).			
4. Attack programs allowing internal access to systems (backdoors visible to internal networks).			
5. Unsecured maintenance modes, developer backdoors.			
6. Modems easily connected, allowing uncontrollable extension of the internal network.			
7. Bugs in network software which can open unknown/unexpected security holes. (Holes can be exploited from external networks to gain access. This threat grows as software becomes increasingly complex.)			
8. Unauthorized physical access to system.			

IMPROVING SECURITY (CONTINUED)

CHECKLIST (CONTINUED)

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
REPUDIATION THREATS 1. Receivers of confidential information may refuse to acknowledge receipt. 2. Senders of confidential information may refuse to acknowledge source. **LEGAL THREATS** 1. Failure to comply with regulatory or legal requirements (e.g., to protect confidentiality of employee data). 2. Liability for acts of internal users or attackers who abuse the system to perpetrate unlawful acts (e.g., incitement to racism, gambling, money laundering, distribution of pornographic or violent material). 3. Liability for damages if an internal user attacks other sites.			